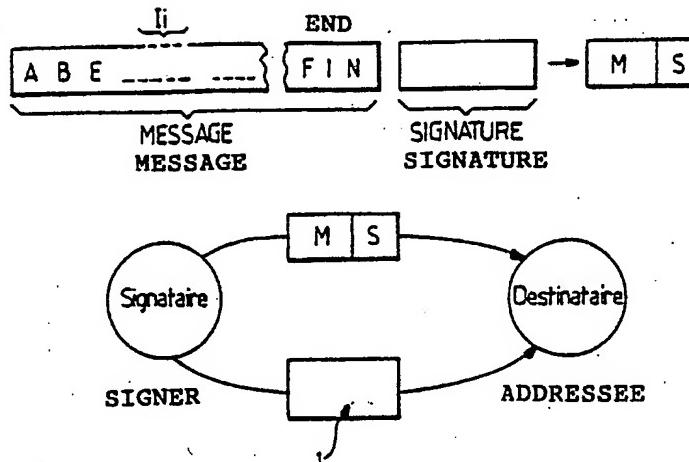




DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁴ : G06F 12/14, G07F 7/10		A1	(11) Numéro de publication internationale: WO 87/05726 (43) Date de publication internationale: 24 septembre 1987 (24.09.87)
<p>(21) Numéro de la demande internationale: PCT/FR87/00079</p> <p>(22) Date de dépôt international: 18 mars 1987 (18.03.87)</p> <p>(31) Numéro de la demande prioritaire: 86/03933</p> <p>(32) Date de priorité: 19 mars 1986 (19.03.86)</p> <p>(33) Pays de priorité: FR</p> <p>(71) Déposant (<i>pour tous les Etats désignés sauf US</i>): INFOS-CRIPT [FR/FR]; 26, rue de Châteaudun, F-75009 Paris (FR).</p> <p>(72) Inventeurs; et</p> <p>(75) Inventeurs/Déposants (<i>US seulement</i>): CAMION, Paul [FR/FR]; 3, rue François Couperin, F-78350 Plaisir (FR). GOUTAY, Jean [FR/FR]; 8/13, parc du Petit Beauregard, F-78170 La Celle St. Cloud (FR). HARARI, Sami [FR/FR]; La Fariede, Près Toulon, 84 (FR).</p>		<p>(74) Mandataire: SCHRIMPFF, Robert; Cabinet Regimbeau, 26, avenue Kléber, F-75116 Paris (FR).</p> <p>(81) Etats désignés: AT (brevet européen), BE (brevet européen), CH (brevet européen), DE (brevet européen), FR (brevet européen), GB (brevet européen), IT (brevet européen), JP, LU (brevet européen), NL (brevet européen), SE (brevet européen), US.</p> <p>Publiée <i>Avec rapport de recherche internationale.</i> <i>Avec revendications modifiées.</i></p>	
<p>(54) Title: METHOD AND DEVICE FOR QUALITATIVE SAVING OF DIGITIZED DATA</p> <p>(54) Titre: PROCEDE ET DISPOSITIF DE SAUVAGARDE QUALITATIVE DE DONNEES NUMERISEES</p> <p>(57) Abstract</p> <p>An encrypted signature (S) representative of the information and of the identity of the holder of those information is established by means of a calculation algorithm for the encryption and the compression of information to be saved. The signature (S) is recorded on the medium carrying the information forming the message (M). The parameters for the calculation of the signature (S), one or several secret keys, are recorded on at least one inviolable carrying medium. Application to the qualitative saving and to the protection of data, on-line or not, of data bases.</p> <p>(57) Abrégé</p> <p>Une signature chiffrée (S) représentative des informations et de l'identité du détenteur de celles-ci est établie au moyen d'un algorithme de calcul de chiffrement et de compression des informations à sauvegarder. La signature (S) est enregistrée sur le support des informations constituant le message (M). Les paramètres de calcul de la signature (S), une ou plusieurs clefs secrètes, sont enregistrés sur au moins un support inviolable. Application à la sauvegarde qualitative et à la protection des données en ligne ou non de bases de données.</p>			



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publant des demandes internationales en vertu du PCT.

AT	Autriche	FR	France	ML	Mali
AU	Australie	GA	Gabon	MR	Mauritanie
BB	Barbade	GB	Royaume-Uni	MW	Malawi
BE	Belgique	HU	Hongrie	NL	Pays-Bas
BG	Bulgarie	IT	Italie	NO	Norvège
BJ	Bénin	JP	Japon	RO	Roumanie
BR	Brésil	KP	République populaire démocratique de Corée	SD	Soudan
CF	République Centrafricaine	KR	République de Corée	SE	Suède
CG	Congo	LI	Liechtenstein	SN	Sénégal
CH	Suisse	LK	Sri Lanka	SU	Union soviétique
CM	Cameroun	LU	Luxembourg	TD	Tchad
DE	Allemagne, République fédérale d'	MC	Monaco	TG	Togo
DK	Danemark	MG	Madagascar	US	Etats-Unis d'Amérique
FI	Finlande				

1

PROCEDE ET DISPOSITIF DE SAUVEGARDE QUALITATIVE DE DONNEES
NUMERISEES

La présente invention est relative à un procédé et à un dispositif de sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable.

5 Avec l'avènement du traitement automatisé de l'information, le problème de la sauvegarde de l'accès aux données traitées ou à traiter s'est tout d'abord posé. Bien que ce problème, notamment en ce qui concerne la protection des données en ligne stockées dans les bases de données des grands systèmes informatiques, ait pu recevoir des solutions efficaces, la mise en oeuvre de ces dernières nécessite l'utilisation de moyens informatiques très importants. Cependant ce type de protection, des intrusions spectaculaires récentes dans des bases de données d'informations concernant la défense de certains états ont pu le révéler, ne peut cependant pas prétendre être absolu. Ce type d'intrusion, mathématiquement et effectivement possible, fait apparaître maintenant un problème d'une autre nature dans la mesure où, ces intrusions sont le plus souvent "transparentes", l'intrus habile pouvant perpétrer son forfait en l'absence de toute trace ou empreinte révélatrice de son identité. Le risque effectivement encouru du fait de telles intrusions comporte non seulement l'accès à des informations confidentielles ou secrètes, à l'insu de l'autorité morale responsable des bases de données correspondantes, dans le cas où l'intégrité qualitative des données est respectée par l'intrus, mais également le risque de la destruction, de la modification en l'absence ou en présence d'intention frauduleuse de l'intrus. En particulier, la presse spécialisée a pu signaler une recrudescence importante

10

15

20

25

30

5 de "détournements de fonds sans effraction matérielle" par simple intrusion dans les banques de données d'organismes financiers ou bancaires et modification et falsification frauduleuse des données de compte de ces établissements.

10 Différents travaux visant à résoudre un problème voisin ont été récemment publiés notamment par la demande de brevet français n° 2 514 593.

15 Selon la technique décrite dans la demande de brevet précitée, un message dont on veut prendre en compte le contenu est tout d'abord soumis à une contraction, cette contraction étant obtenue par un traitement de type code de Hamming. Une signature est ensuite calculée sur la contraction obtenue au moyen d'un algorithme de chiffrement, la signature chiffrée présentant un nombre de chiffres ou caractères identiques au nombre de chiffres ou caractères de la contraction.

20 Cependant la technique décrite dans la demande de brevet précitée ne peut prétendre être utilisée en vue d'effectuer une sauvegarde qualitative de données numérisées telles que celles contenues dans une base de données au double motif ci-après.

25 La contraction du message initial par un traitement linéaire tel que le code de Hamming ne peut en aucune façon prétendre constituer une représentation unique du message initial, plusieurs messages différents pouvant engendrer la même contraction. La sauvegarde qualitative de textes quelconques n'est donc 30 pas possible puisque en définitive, deux messages différents peuvent ainsi produire la même contraction et donc la même signature.

En outre, la séquence de chiffrement de la contraction pour l'élaboration de la signature chiffrée étant réalisée au sein des circuits d'une carte à mémoire protégée, dont la capacité de calcul est modeste, la contraction et la signature chiffrée ne peuvent au plus comporter que six caractères.

La présente invention a pour but de remédier aux inconvenients précités en vue, notamment, une protection absolue de l'accès aux données en ligne des banques de données ne pouvant être totalement garantie, d'assurer un moyen de conservation de l'intégrité de données numérisées par une sauvegarde qualitative de ces données enregistrées sur un support effaçable ou modifiable.

Un autre objet de la présente invention est la mise en oeuvre d'un procédé et d'un dispositif de sauvegarde qualitative de données numérisées dans lesquels une signature parfaitement représentative d'un texte ou message unique et de son auteur signataire est apposée sur le support sur lequel les données sont enregistrées en clair, la signature constituant un sceau.

Un autre objet de la présente invention est la mise en oeuvre d'un procédé et d'un dispositif de signature, chaque texte, différent, ayant une signature pour une clef déterminée, cette signature étant indépendante du texte de départ.

Un autre objet de la présente invention est également, dans le cas de transmission d'informations signées conformément à la présente invention par un détenteur signataire, la possibilité pour l'utilisateur destinataire d'une authentification tant de

l'intégrité des informations transmises que de l'origine de celles-ci.

Un autre objet de la présente invention est également, par la mise en oeuvre du procédé et du dispositif de l'invention relativement à une pseudo-information, la définition entre signataire de la pseudo-information et destinataire d'un code d'accès aléatoire temporaire.

Le procédé de sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable, objet de l'invention, est remarquable en ce qu'il consiste à établir une signature chiffrée représentative des informations et de l'identité du détenteur de ces informations au moyen d'un algorithme de calcul et à enregistrer celle-ci sur le support des informations. Les paramètres de calcul de la signature sont enregistrés sur au moins un support inviolable.

Le dispositif pour la sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable, objet de l'invention, est remarquable en ce qu'il comprend des premiers moyens de mémorisation dans lesquels sont mémorisées la ou les clefs secrètes du détenteur signataire ou du destinataire des informations et des deuxièmes moyens de mémorisation dans lesquels est mémorisé un programme de calcul d'une ou plusieurs signatures conformément au procédé de l'invention. Des moyens de calcul de la ou des signatures et des moyens d'inscription de cette ou ces signatures sur le support des informations à sauvegarder sont prévus. Des moyens

de comparaison de la signature (S,Sc) inscrite sur le support des informations avec la signature calculée et des moyens de validation d'utilisation des informations sauvegardées sur coïncidence de la signature (S,Sc) calculée et de la signature enregistrée sur le support d'enregistrement des informations (Ii) sont en outre prévus. Des moyens périphériques de saisie ou de visualisation des données permettent un dialogue interactif entre système et utilisateur signataire ou destinataire des données.

L'invention trouve application ainsi qu'il sera décrit en détail dans la suite de la description à l'échange de données numériques entre utilisateurs, à la protection de fichiers entrés localement, à la protection contre les doubles lectures de données sur identification du demandeur, à la gestion des programmes distribués sur réseau à des terminaux localement programmables, à la gestion de la maintenance pour progiciel, à la gestion de fichiers internes au cours d'utilisation périodique de ceux-ci, à la vérification des opérations comptables ou de gestion, à l'archivage des informations comptables ou bibliographiques, à la conservation de bibliothèques de programmes, de copies de sécurité de bases de données, de fichiers conservés en local et en central par calcul et comparaison des signatures correspondantes.

Elle sera mieux comprise à la lecture de la description et à l'observation des dessins ci-après dans lesquels :

- La figure 1 représente de manière schématique des éléments essentiels permettant la mise en oeuvre du procédé objet de l'invention,

5 - la figure 2 représente, de manière schématique, un mode de réalisation particulièrement avantageux d'un moyen permettant la mise en oeuvre du procédé objet de l'invention,

10 - la figure 3 représente un schéma illustratif du procédé de sauvegarde qualitative d'informations, objet de l'invention, dans le cas où les informations sont transmises d'un signataire à un destinataire,

15 - la figure 4 représente schématiquement un mode de réalisation particulièrement avantageux d'un algorithme de calcul de la signature conformément au procédé de l'invention,

20 - la figure 5 représente une variante de réalisation de mise en oeuvre de l'algorithme de calcul, tel que représenté en figure 4,

25 - la figure 6 représente une autre variante de réalisation et de mise en oeuvre d'un algorithme de calcul de la signature, tel que représenté en figure 4, dans le cas où un grand nombre d'informations à sauvegarder constituant le message ou texte est prévu,

30 - la figure 7 représente schématiquement une variante de mise en oeuvre du procédé de sauvegarde qualitative, objet de l'invention, cette variante étant particulièrement avantageuse en vue d'obtenir une hiérarchisation successive des signatures pour un texte ou message considéré,

35 - la figure 8 représente un schéma synoptique d'un dispositif permettant la mise en oeuvre du procédé objet de l'invention, ce dispositif étant

particulièrement adapté à la mise en œuvre du procédé objet de l'invention,

5 - la figure 9 représente une variante de réalisation du dispositif pour la sauvegarde qualitative d'informations numérisées enregistrées dans le cas où la quantité d'informations constitutives du message est relativement réduite et où une utilisation domestique peut être envisagée,

10 - la figure 10 représente enfin un organigramme des fonctions du dispositif pour la sauvegarde qualitative d'informations numérisées objet de l'invention, tel que représenté précédemment en figures 8 ou 9.

15 Le procédé de sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable, objet de l'invention, sera tout d'abord décrit en liaison avec les figures 1 et 2.

Conformément à la figure 1, le procédé de sauvegarde qualitative d'informations, objet de l'invention, consiste à établir une signature chiffrée, notée S, représentative des informations et de l'identité du détenteur de ces informations au moyen d'un algorithme de calcul. La signature S est enregistrée sur le support des informations, les informations constituant un texte ou un message. Le message ou texte est par exemple enregistré en clair, afin d'assurer la sauvegarde du message ou du texte ou la transmission de celui-ci. Par enregistrement en clair du message ou du texte sur le support effaçable ou modifiable, on entend bien entendu que celui-ci est enregistré sur ce support en l'absence de tout chiffrement ou de tout codage quelconque visant à en dissimuler la signification.

Les paramètres de calcul de la signature S sont enregistrés sur au moins un support inviolable.

Ainsi qu'il a été représenté en figure 2, le support inviolable peut avantageusement être constitué par une carte à mémoire protégée. Sur la figure 2 on a représenté la carte à mémoire protégée, de manière schématique, celle-ci étant réputée comporter en 10 une zone active constituée par exemple par un microprocesseur intégré à la carte, en 11 une zone secrète totalement inaccessible, protégée par le microprocesseur 10, en 12 une zone protégée en lecture et en écriture et accessible seulement suite à introduction d'un code donné, et en 13 une zone totalement libre à l'écriture et à la lecture. Sur la figure 2, la carte à mémoire est référencée 1. Les cartes à mémoire protégées sont normalement disponibles dans le commerce et on pourra se reporter utilement aux demandes de brevet français n° 74 10191 et leur addition 75 08184 et 75 08185 délivrées le 10 Mars 1980 pour une description plus détaillée de dispositifs tels que des cartes à mémoire protégée.

Conformément au procédé objet de l'invention, l'algorithme de calcul est avantageusement un algorithme de chiffrement du message ou texte à sauvegarder, et de compression des informations contenues dans le texte à sauvegarder à partir d'au moins une clef secrète associée au signataire détenteur des informations.

Bien entendu, l'algorithme de chiffrement et de compression des informations notées II sur la figure 1 est choisi de façon à assurer une indépendance relative entre tout texte déterminé et la signature.

S engendrée à partir de ce texte. Par indépendance relative entre le contenu du texte ou message et la signature calculée au moyen de l'algorithme conformément à la présente invention, on comprendra, d'une part, que pour un texte donné une seule signature S est obtenue et que d'autre part, toute modification la plus minime au niveau de l'information II contenue dans le message ou dans le texte a pour effet d'engendrer une signature S différente de la signature d'origine en l'absence de corrélation apparente.

Un exemple d'utilisation particulièrement avantageux du procédé de sauvegarde qualitative d'informations numérisées conforme à la présente invention sera décrit en liaison avec la figure 3.

Conformément à cette figure, et notamment en vue d'assurer la transmission des informations sauvegardées conformément au procédé objet de l'invention, les informations devant être transmises à un destinataire, le procédé objet de l'invention consiste à adresser le support inviolable 1 sur lequel les paramètres de calcul de la signature chiffrée S ont été enregistrés au destinataire, puis à transmettre les informations sauvegardées sur le support et la signature chiffrée S au destinataire. Le destinataire étant en possession du support inviolable 1 qui lui a été adressé par toute voie, ainsi que du message M et de sa signature S, il peut alors en vue de contrôler le contenu des données transmises et reçues et à partir des paramètres de calcul de la signature S contenus dans le support inviolable 1, établir une signature chiffrée de contrôle S', à partir des informations sauvegardées reçues, suite à la transmission. Il peut

ensuite comparer la signature chiffrée reçue par transmission, notée S, et la signature chiffrée de contrôle notée S'. L'identité des informations sauvegardées et des informations reçues par le destinataire et l'origine authentifiée de ces informations est alors obtenue à la coïncidence de la signature chiffrée S et de la signature chiffrée de contrôle S'.

Bien entendu, la clef secrète ou les clefs secrètes constituant au moins une partie des paramètres de calcul de la signature S sont enregistrées dans la zone protégée secrète inaccessible 11 de la carte à mémoire 1 ou support inviolable, celui-ci ayant été mis à disposition du destinataire et éventuellement même du signataire. Les supports de mémorisation inviolables tels que les cartes à mémoire constituent actuellement des supports dont le caractère d'inviolabilité est actuellement le meilleur. En effet, la structure mécanique de ce type de composant électronique et la protection des mémoires intégrées à ce composant par un microprocesseur en ce qui concerne l'accès à celles-ci, permet de s'assurer d'un haut niveau de protection.

Cependant, la mise en oeuvre du procédé objet de l'invention n'est pas limitée à l'utilisation de support de mémorisation inviolable tel que des cartes à mémoire protégée. En effet, on peut bien entendu envisager la mise en oeuvre du procédé à l'aide de moyens dans lesquels le support inviolable peut être constitué par tout circuit protégé activement en ce qui concerne l'accès aux zones mémorisées par un micro-

processeur ou analogue, et structurellement par tout moyen adapté.

5 Un mode de mise en oeuvre du procédé de sauvegarde qualitative d'informations numérisées conformément à l'invention sera maintenant décrit en liaison avec les figures 4 à 7.

Conformément à une caractéristique avantageuse du procédé objet de l'invention, la clef secrète et la signature S peuvent être constituées par un mot comprenant un nombre de caractères ou chiffres identiques. La signature et/ou la ou les clefs secrètes peuvent être constituées par un mot comprenant également des caractères alpha-numériques. Ainsi, pour un mot comprenant n caractères, tels que par exemple des caractères alpha-numériques définis par le code ASCII étendu, lequel comprend 256 caractères, la probabilité d'obtention de la ou des clefs secrètes ou éventuellement, pour la mise en oeuvre de texte différent, d'une même signature S est de l'ordre de 20 $(\frac{1}{256})^n$ ou au plus égale à $(\frac{1}{10})^n$ lorsque des chiffres sont utilisés.

Ainsi qu'il est en outre représenté en figure 4, en vue d'établir la signature chiffrée S représentative des informations et de l'identité du détenteur des informations, l'algorithme de calcul permettant d'effectuer le chiffrement des informations notées II puis la compression de ces informations, peut consister, selon un mode de réalisation avantageux, à initialiser la création d'une suite de nombres aléatoires ou pseudo-aléatoires à plusieurs chiffres, à partir de la ou des clefs secrètes.

Sur la figure 4, les informations I_i sont notées DBA et ainsi de suite, et les nombres aléatoires ou pseudo-aléatoires à plusieurs chiffres sont notés C_i . On a ainsi représenté N nombres aléatoires
5 sur cette figure.

Conformément à une caractéristique particulièrement avantageuse de l'objet de l'invention, la suite de nombres aléatoires notés C_i comporte un même nombre de termes C_i , ou un diviseur de ce nombre, que le nombre de caractères I_i de l'information à sauvegarder. Conformément au procédé objet de l'invention, l'algorithme de chiffrement permet alors d'effectuer le produit scalaire, noté P, terme à terme de la suite de nombres aléatoires C_i et de l'information à sauvegarder I_i .

15 Le produit scalaire ainsi obtenu est noté

$$P = \sum_{i=1}^N I_i * C_i$$

20 L'algorithme de calcul permet alors d'effectuer une réduction modulaire du produit scalaire P modulo p de façon à définir un nombre $A = P$ modulo p où A représente le reste de la division de P par p, dans lequel p est un nombre premier comportant un nombre de chiffres égal au nombre de caractères de la ou des clefs secrètes ou de la signature S. L'algorithme de calcul permet ensuite d'effectuer une exponentiation modulaire du nombre A de façon à définir un nombre S = $A * e^d$ modulo q, où S représente le reste de la division de $A * e^d$ par q, dans lequel q est un nombre premier comportant un nombre de chiffres égal au nombre de caractères de la ou des clefs secrètes ou de la signature et où d représente un ou plusieurs chiffres consécutifs ou non de la ou des clefs secrètes.
25
30

Le nombre S ainsi obtenu constitue la signature chiffrée.

Afin d'augmenter la solidité cryptographique de la signature chiffrée S, il est également possible, conformément au procédé objet de l'invention, d'ajouter au produit scalaire P une valeur aléatoire produit de nombres supplémentaires aléatoires ou pseudo-aléatoires notés CN + k sur la figure 5, et de valeurs numériques arbitraires notées AN + k sur cette même figure, valeurs telles que la date, l'heure, un numéro d'identification du détenteur d'informations ou un code d'identification de ce demandeur consistant par exemple en des caractères alpha-numériques, ou éventuellement un nombre aléatoire d'un ou plusieurs chiffres.

Bien entendu, aux caractères Ii de l'information à sauvegarder, peuvent être ajoutées, par concaténation, des chaînes de caractères représentatives de valeurs numériques significatives arbitraires, telles que la date, l'heure, un numéro d'identification ou code d'identification du détenteur d'informations ou un nombre aléatoire ainsi que précédemment cité. Dans ce cas, ces informations supplémentaires sont directement intégrées à l'information notée ΣI_i à sauvegarder. Bien entendu, la suite de nombres pseudo-aléatoires Ci est alors complétée par des nombres aléatoires notés CN + k complétant la suite.

Le procédé objet de l'invention tel que décrit précédemment peut avantageusement être mis en oeuvre dans le cas où le texte ou message à sauvegarder qualitativement comporte par exemple 250 caractères alpha-numériques. Dans ce cas, et pour les applications les plus courantes, la signature S et la ou les clefs secrètes peuvent alors comporter par exemple six carac-

teres ou chiffres décrits.

Cependant, le procédé de sauvegarde qualitatif d'information numérisée objet de l'invention, n'est pas limité à un tel nombre de caractères constituant le message ou texte. Bien entendu, il peut avantageusement être utilisé dans le but de sauvegarder qualitativement des informations de banques de données, le nombre de caractères de ces informations pouvant atteindre plusieurs milliers. Dans ce cas, il est avantageux d'utiliser pour la mise en œuvre du procédé, un ordinateur de grande capacité de calcul, afin d'obtenir des temps de calcul minimum pour le calcul des signatures S.

Dans le cas précédemment décrit, les informations à sauvegarder I_i et les nombres aléatoires C_i peuvent avantageusement être subdivisés en blocs de données notés B_j , ainsi qu'il est représenté en figure 6. Les blocs B_j contiennent un nombre déterminé Q de caractères et le produit scalaire P est calculé de manière avantageuse pour chacun des blocs B_j , de façon à définir des produits scalaires partiels notés P_j . Bien entendu, les produits scalaires partiels P_j sont de la forme :

$$P_j = \sum_i^Q I_{ij} * C_i$$

25

Ainsi, une signature partielle notée S_j est calculée pour chacun des blocs B_j et la suite des signatures S_j constitue la signature finale représentative de l'ensemble des informations à sauvegarder.

30

Ainsi qu'il apparaît en outre en figures 1 à 6, les nombres aléatoires ou pseudo-aléatoires C_i constituant les suites de nombres aléatoires sont avantageu-

sement des nombres comportant un nombre l de chiffres ou caractères égal au nombre de caractères de la ou des clefs utilisées. De manière avantageuse mais non limitative, les caractères i de l'information à sauvegarder peuvent être groupés de façon que le nombre de chiffres de chaque terme C_i de la suite de nombre aléatoires soit supérieur au nombre de caractères constituant un groupement. On comprendra bien sûr que les caractères constituant l'information à sauvegarder, le caractère noté I_i , sont enregistrés sous forme numérisée, c'est-à-dire en fait sous forme de bits d'informations zéro ou 1. Dans ce cas, une pluralité de bits constituant la représentation totale ou partielle d'un caractère peut être groupée de façon à constituer un groupement tel que défini précédemment. Le produit terme à terme des groupements ou caractères et des nombres constituant les nombres aléatoires ou pseudo-aléatoires de la suite de nombres notés C_i s'entend comme le produit arithmétique de tout groupement ou caractère d'ordre i correspondant.

Une variante particulièrement avantageuse du procédé de sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable sera décrit maintenant en liaison avec la figure 7.

Selon la figure précitée, le procédé conformément à l'invention, consiste pour une même quantité d'informations à sauvegarder, quantité d'informations notée ΣI_i correspondant à une longueur de texte ou de message donné, à calculer de manière itérative une pluralité notée r de signatures, elles-mêmes notées S_K , successives. Bien entendu, les signatures S_K sont calculées à partir de l'algorithme de calcul tel que

précédemment décrit par exemple. Conformément à un mode de réalisation avantageux du procédé de l'invention, les signatures notées S_{K-1} sont successivement intégrées, comme chaîne de caractères, à l'information à sauvegarder ΣI_i . Les signatures peuvent par exemple être intégrées par concaténation aux informations ΣI_i . Suite à l'intégration d'une signature d'ordre $K-1$, aux informations ΣI_i précitées, une signature d'ordre supérieure S_K est alors calculée 5 à nouveau sur l'ensemble des informations à sauvegarder auxquelles ont été ajoutées les signatures d'ordre inférieur considérées comme chaîne de caractères. On obtient ainsi une définition particulièrement intéressante de signatures successives permettant une hiérarchisation des signatures et notamment de la signature finale notée S_K , à partir des signatures d'ordre inférieur S_0, S_{K-1} , pour un même contenu d'informations notées ΣI_i . Bien entendu, dans ce cas, la signature S_K 10 finale constitue en fait la signature S au sens du procédé objet de l'invention ou une signature à haut degré de hiérarchie.

15

20

Une autre variante particulièrement avantageuse du procédé de sauvegarde qualitative de l'information numérisée, objet de l'invention, peut consister préalablement à l'inscription sur le support des informations I_i ou sur le support inviolable de la signature S à soumettre en outre la signature S précitée à un traitement de chiffrement à partir, par exemple, d'une clef secrète de chiffrement, de façon à obtenir une 25 signature chiffrée notée S_c . Le traitement de chiffrement sur la signature S peut être réalisé à partir 30 d'un programme de calcul de chiffrement de type classique, tel que par exemple un programme de calcul connu sous le nom de programme ou méthode DES. Dans ce cas, la signature est chiffrée S_c et présente un

nombre de caractères identique à celui de la signature S. Le traitement de chiffrement peut bien entendu être appliqué soit à la signature S obtenue par simple application du procédé objet de l'invention, 5 tel que déjà décrit, ou suite à une application itérative du procédé, la signature S considérée étant alors la dernière obtenue d'ordre K ainsi que déjà décrit précédemment.

Dans le cas où la signature S soumise au traitement de chiffrement précité comporte un nombre de caractères limité à six pour l'application particulière précédemment décrite, le traitement de chiffrement peut avantageusement être alors réalisé au niveau des circuits du support inviolable, lorsque celui-ci est 10 constitué par une carte à mémoire. Dans ce cas, la signature chiffrée obtenue et calculée par le microprocesseur de la carte à mémoire 1 est alors transférée pour inscription sur le support des informations II. L'élaboration d'une signature chiffrée Sc 15 permet d'obtenir bien entendu, une amélioration de la solidité cryptographique de la signature ainsi traitée. 20

Une description plus complète d'un dispositif permettant la mise en œuvre du procédé objet de l'invention pour la sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable, sera maintenant donnée en liaison avec les figures 8 à 10.

Ainsi qu'il apparaît en figure 8, le dispositif permettant d'assurer la sauvegarde qualitative d'informations numérisées, objet de l'invention, comporte des premiers moyens de mémorisation notés 101, dans lesquels sont mémorisées la ou les clefs secrètes du détenteur signataire ou du destinataire des informa-

tions IIi constituant le texte ou message à sauvegarder. Des deuxièmes moyens 102 de mémorisation sont également prévus dans lesquels est mémorisé un programme de calcul d'une ou plusieurs signatures S, Sc, conformément au procédé tel que décrit précédemment dans la description. Des moyens de calcul notés 103 de la ou des signatures S, Sc et d'inscription 104 de ces signatures S, Sc sur le support des informations IIi à sauvegarder sont également prévus. Des moyens de comparaison 105 de la signature S ou Sc inscrites sur le support des informations avec la signature calculée sont également prévus et des moyens de validation 106 permettent de valider l'utilisation des informations sauvegardées sur coïncidence de la signature S ou Sc calculée et de la signature enregistrée sur le support d'enregistrement des informations IIi. Bien entendu, des moyens périphériques notés 107 de saisie et/ou de visualisation des données sont également prévus, afin d'assurer un dialogue interactif avec l'utilisateur.

On comprendra en particulier que le dispositif tel que décrit en figure 8 peut aussi bien être utilisé par le détenteur signataire des informations à sauvegarder que par le destinataire de ces informations sauvegardées, celui-ci devant alors procéder à une vérification pour authentification de signature, permettant en celà l'authentification des données reçues.

Les premiers et deuxièmes moyens de mémorisation 101 et 102 sont constitués par des supports de mémorisation inviolables. On comprendra bien entendu que le dispositif objet de l'invention tel que représenté en figure 8 peut être constitué par un ordinateur ou un

microordinateur. Dans le cas où les indications à sauvegarder sont constituées par une très grande quantité d'informations, telles que des informations comptables, l'ordinateur peut avantageusement être constitué par un ordinateur de grande capacité de calcul, tel qu'un ordinateur IBM 30 - 33 permettant d'opérer 4,8 millions d'instructions par seconde.

5 Dans ce cas, le nombre de caractères de la signature pourra être avantageusement porté à 24 et une procédure de traitement par blocs d'informations notés Bj pourra avantageusement être utilisée. Le langage de programmation permettant la réalisation des programmes de calcul correspondant pourra par exemple être le langage COBOL. Au contraire dans le cas où

10 le nombre ou quantité d'informations à traiter, c'est-à-dire, pour des textes ou messages de longueur beaucoup plus réduite, sera envisagé, un micro-ordinateur normalement disponible dans le commerce, pourra être utilisé. Dans ce cas, le langage de programmation pourra avantageusement être constitué par un langage d'assemblage. En outre, les supports de mémorisation constituant les premiers et deuxièmes moyens de mémorisation 101, 102, peuvent être constitués par des supports de mémorisation inviolables.

15 Sur la figure 8, le caractère d'inviolabilité des supports 101, 102 est représenté par des hachures entourant les éléments 101, 102. Dans le cas d'ordinateurs ou même de micro-ordinateurs, les zones mémoires correspondantes pourront être munies de structures adaptées à en assurer l'inviolabilité.

20 Cependant, les supports de mémorisation inviolables pourront également être constitués par des cartes à

25

30

mémoire protégée. Ce mode de réalisation apparaît particulièrement avantageux en particulier dans le cas où le dispositif est constitué par exemple par un micro-ordinateur, les micro-ordinateurs comportant un lecteur de carte à mémoire protégée, tendant à constituer actuellement une nouvelle norme de commercialisation.

Bien entendu, la réalisation d'un dispositif conforme à l'invention au moyen d'un micro-ordinateur n'est pas indispensable et il pourra être avantageux de réaliser le dispositif objet de l'invention à l'aide de composant ou système électronique moins onéreux, en vue d'utilisations domestiques ou d'utilisations pour lesquelles la quantité d'informations ou les messages ou textes est plus faible.

Dans le cas précédemment cité, le dispositif permettant la mise en oeuvre du procédé objet de l'invention peut avantageusement comporter en vue de constituer des moyens périphériques un terminal de visualisation du genre "Minitel" distribué par l'Administration des Postes et Télécommunications. Sur la figure 9, un tel dispositif a été représenté et le terminal de visualisation "Minitel" a été référencé 200. Conformément à cette figure, le dispositif objet de l'invention comprend en outre un lecteur de cartes à mémoire protégée noté 201, le lecteur comportant une fente notée 202 d'introduction de cartes à mémoire 1. Le lecteur de cartes à mémoire protégée 201 est également avantageusement muni d'une cartouche enfichable 203 comportant des mémoires mortes dans lesquelles est stocké le programme de calcul de la signature ou des signatures S, Sc. La cartouche enfichable 203 peut avantageusement être enfichée dans un logement d'in-

sertion 204 prévu dans le lecteur de cartes 201.

Le lecteur de cartes à mémoire 201 est en outre équipé d'un microprocesseur 205, celui-ci ayant pour rôle d'assurer le chargement des programmes emmagasinés dans la cartouche 203 et le chargement des données secrètes mémorisées dans la carte à mémoire 1. La liaison avec le terminal du type Minitel 200 est assurée par câble 206.

En outre, la signature S étant soumise à un traitement de chiffrement conformément au procédé tel que précédemment décrit, un programme de chiffrement peut être mémorisé dans les zones protégées du support de mémorisation inviolable 11 de la carte à mémoire 1, le calcul de chiffrement de la signature S étant alors réalisé au sein de la carte à mémoire 1.

Afin d'assurer au système une convivialité de haut niveau vis-à-vis de l'utilisateur, que celui-ci soit le détenteur des informations signataires ou le destinataire de ces informations, le dispositif objet de l'invention comporte en mémoire permanente un programme de gestion de type "menu" permettant sur incitation de l'utilisateur, par affichage de pages écran de dialogue interactif, la réalisation d'une pluralité de fonctions, lesquelles seront décrites en liaison avec la figure 10.

Le programme de type "menu" précité permet tout d'abord en 1000 d'introduire le code personnel de l'utilisateur signataire ou destinataire. Puis il permet en outre d'introduire en 1001 des paramètres arbitraires ou aléatoires tels que la date, l'heure ou des chiffres aléatoires. Bien entendu, l'introduction de ces paramètres peut être remplacée par la production par le système de ces paramètres, en

particulier lorsque le système dans le cas d'un micro-ordinateur notamment ou d'un ordinateur est muni d'une horloge interne à partir de laquelle les paramètres de date et d'heure peuvent être directement introduits. En outre, le programme "menu" permet également l'introduction du message ou du texte à sauvegarder, cette opération étant notée en 1002. Bien entendu, l'introduction de la ou des clefs secrètes et de l'identifiant du signataire par exemple est effectuée en 1003. On notera que dans le cas où une carte à mémoire est utilisée, l'introduction de la ou des clefs secrètes et de l'identifiant du signataire en 1003 est effectuée au moyen du support inviolable tel qu'une carte à mémoire protégée, l'introduction de la ou des clefs secrètes mémorisée dans la zone protégée de la carte à mémoire 1 peut par exemple être effectuée après insertion de la carte 1 dans le lecteur 201 sur simple introduction du code personnel de l'utilisateur au clavier du système lecteur de cartes, la ou les clefs secrètes introduites étant bien entendu inconnues elles-mêmes de l'utilisateur. Dans ce cas, l'utilisateur destinataire est bien sûr titulaire d'une même carte à mémoire dans laquelle les codes et/ou les paramètres de calcul de la signature ou des signatures sont également mémorisés. Dans le cas où, au contraire, le dispositif ne comporte pas de système de lecteur de cartes à mémoire 201, il est bien entendu toujours possible d'introduire directement les clefs secrètes et les paramètres de calcul de la signature directement au clavier constituant périphériques du dispositif. Bien entendu, le degré de sécurité requis imposera les

solutions les plus adaptées.

Le déroulement du programme de calcul de chiffrement et de compression modulaire, tel que précédemment décrit dans la description est alors effectué par l'intermédiaire du microprocesseur, du micro-ordinateur ou du lecteur de cartes 201 associé à un terminal de visualisation, ou, enfin, par l'unité centrale de l'ordinateur. Sur la figure 10, le calcul de la signature est représenté aux étapes 1004 et 1005.
Suite à l'obtention de la signature S ou de toute signature telle que précédemment définie dans la description, l'affichage et l'inscription sur le support des informations et/ou sur le support inviolable est réalisé à l'étape 1006.
En outre, ainsi qu'il apparaît en figure 10, le programme de gestion de type menu permet également à un utilisateur destinataire d'introduire la signature à vérifier pour comparaison à la signature stockée ou transmise. Une comparaison de la signature S inscrite sur le support des informations II et de la signature de contrôle S' est alors effectuée, les opérations précitées étant représentées en 1007 sur la figure 10. En cas de coïncidence de la signature de contrôle S' et de la signature S, le dispositif procède alors à une validation de signature et des informations transmises en 1008.

Ainsi qu'il apparaît en outre en figure 10, dans le cas où une invalidation de signature est obtenue à l'étape 1009, les pages écran comportent une page écran de signalisation de risque de destruction des zones mémoires du support inviolable après un nombre déterminé d'essais infructueux de validation de signature.

Les pages écran précitées sont représentées par exemple en 1011, après une étape de comptabilisation du nombre d'essais infructueux représentée en 1010.

On comprendra bien entendu que les procédures de signature et de validation de signature mises en oeuvre par le dispositif précédemment décrit, sont séparées. La procédure de validation de signature est conditionnellement autorisée pour des codes d'identification de l'utilisateur identifiant, donc l'utilisateur destinataire, distincts des codes d'identification de l'utilisateur signataire. Ainsi, cette procédure permet à l'utilisateur identifiant destinataire de vérifier des signatures qu'il ne peut pas lui-même écrire. La seule connaissance requise à l'utilisateur identifiant destinataire pour assurer cette opération est par exemple le code personnel, consistant par exemple en des caractères alpha-numériques, du détenteur d'informations ou signataire.

Une autre application particulièrement intéressante du procédé et du dispositif objet de l'invention sera maintenant décrite également en liaison avec la figure 10. Conformément à un aspect particulier du dispositif et du procédé objet de l'invention, pour un nombre aléatoire d'identification déterminé introduit en 1001 par l'utilisateur, lequel possède le code de ce nombre aléatoire d'identification, l'introduction d'une pseudo-information à sauvegarder en 1002, pseudo-information consistant en une répétition à l'identique de caractères II déterminés sur un nombre arbitraire de caractères, permet d'engendrer un code d'accès aléatoire inviolable temporaire représentatif de cet utilisateur. Sur transmission du code d'identi-

fication et du nombre aléatoire d'identification à un utilisateur récepteur, la procédure de validation du code d'accès aléatoire inviolable temporaire est alors autorisée.

5 On comprendra bien entendu que la pseudo-information peut consister en n'importe quel caractère arbitraire, tel que par exemple un caractère alpha-numérique du code ASCII étendu et notamment en un espacement, celui-ci étant susceptible de procurer
10 la probabilité d'erreur minimum pour la phase d'introduction d'un message ou de texte relatif à la pseudo-information.

On comprendra alors que le code d'accès aléatoire inviolable temporaire représentatif de l'utilisateur consiste bien entendu en la signature calculée sur la pseudo-information à laquelle a été ajouté, par concaténation, le nombre aléatoire d'identification introduit par l'utilisateur. Le procédé ainsi utilisé est particulièrement avantageux en ce qu'il permet bien
20 entendu pour un organisme serveur, tel qu'une base de données, l'identification de tout abonné, à partir de codes aléatoires temporaires représentatifs de cet abonné. Ainsi, l'accès au serveur ou à la base de données correspondante est protégé par un système de code
25 d'accès totalement renouvelable et pour lequel la période de renouvellement peut être prise arbitrairement à l'initiative de l'organe serveur. On comprendra en effet que le changement du caractère répété à l'identique à l'initiative de l'organe serveur permet en fait de provoquer
30 un changement complet du pseudo-texte ou pseudo-informations nécessaire pour engendrer le code d'identification ou d'accès.

Le procédé et le dispositif objet de l'invention apparaissent ainsi particulièrement avantageux en ce qu'ils permettent d'une part la protection de l'accès à un organisme serveur et également la sauvegarde qualitative des données numérisées enregistrées sur support effaçable ou modifiable de cet organisme serveur lorsque ces données sont en ligne, par constitution d'une bibliothèque de référence.

Les applications du procédé et du dispositif objet de l'invention ne sont cependant pas limitées à cette seule utilisation.

Ainsi, le procédé et le dispositif objet de l'invention peuvent avantageusement être utilisés pour l'échange de données avec l'extérieur, le destinataire des informations, en conservant les sceaux déjà vérifiés, évitant aisément les doubles lectures. En outre, dans le cas de réseau de terminaux éloignés, la signature peut être utilisée pour protéger des fichiers entrés localement. Il est en effet facile de vérifier que le signataire est bien habilité dans les payes, les facturations ou analogues auprès de l'ordinateur central et que les données n'ont pas été altérées. La signature peut également être utilisée en vue d'assurer la prévention contre les doubles lectures, en ce cas, la signature est seulement comparée avec les signatures précédemment calculées. En cas de coïncidence de signature, celle-ci témoigne de l'existence d'une lecture du fichier correspondant.

Le procédé et le dispositif objet de l'invention peuvent en outre être utilisés avantageusement pour la gestion de programmes distribués. En effet, dans un réseau contenant des terminaux locaux programmables,

l'ordinateur central doit pouvoir s'assurer que tous les terminaux ont des copies à jour des programmes corrects. Une telle vérification peut être effectuée par envoi périodique d'une clef, par l'ordinateur central à chaque terminal. Chacun de ces derniers calcule alors un nouveau sceau ou signature à partir du texte du programme et de la nouvelle clef. Sur transmission par chaque terminal de cette nouvelle signature à l'ordinateur central, celui-ci le compare au sceau calculé pour chacun des terminaux, à partir du texte du programme de référence. Sur identité des signatures ou sceaux, les programmes seront considérés comme identiques.

En outre, le procédé et le dispositif objet de l'invention permettent de s'assurer de l'absence d'erreurs au niveau des progiciels diffusés auprès d'une nombreuse clientèle. Dans ce but, le prestataire diffusant le logiciel peut comparer le sceau du progiciel qui a été placé à l'origine auprès de la clientèle avec celui du programme réel, afin de prouver l'existence ou la non existence d'erreurs ou modifications.

Le procédé et le dispositif objet de l'invention peuvent également être utilisés avantageusement pour vérifier qu'aucun changement n'a pu être effectué sur des fichiers entre plusieurs utilisations périodiques de ces fichiers. De la même façon, la vérification de totaux de contrôle, de décomptes comptables ou financiers peuvent être effectués. Dans ce cas, l'utilisation du procédé et du dispositif objet de l'invention permettent de garantir qu'il n'y a pas eu de manipulations volontaires ou même d'erreurs involontaires dans les décomptes précités.

Une autre application particulièrement intéressante du procédé et du dispositif objet de l'invention consiste dans l'archivage d'informations, telles que des informations comptables. En effet, 5 certaines lois nationales exigent que les informations comptables soient archivées pendant un temps déterminé, dix ans le plus souvent. Bien entendu, ces lois nationales exigent également des conditions 10 pleinement satisfaisantes relativement à la sécurité de maintien de l'intégrité de l'information. L'archivage magnétique étant autorisé, la méthode et le dispositif objet de l'invention pourront avantageusement être utilisés pour vérifier que ces informations sont restées intactes et sans modification, 15 même après de nombreuses années d'archivage.

En outre, le procédé et le dispositif objet de l'invention peuvent avantageusement être utilisés afin d'attribuer à chaque copie de sauvegarde des informations des bases de données, pour attribuer à 20 ces dernières un sceau ou signature absolument représentatif du contenu de ces copies. Ainsi lorsqu'il est nécessaire d'utiliser les copies munies de leur sceau ou signature pour reconstituer l'information d'une base de données endommagée, la signature peut 25 être vérifiée avant rechargement.

Enfin, le procédé et le dispositif objet de l'invention peuvent être utilisés pour s'assurer de l'identité à une date déterminée de fichiers utilisés par des filiales d'une même société localement et 30 centralement. Dans ce cas, le calcul et la comparaison des seuls sceaux ou signatures correspondant au fichier permettent d'assurer et de garantir l'iden-

tité de ce fichier.

Bien entendu, le procédé et le dispositif objet de l'invention ne sont pas limités à la sauvegarde qualitative d'informations numérisées. Ils peuvent avantageusement être utilisés pour la génération ou création de clés chiffrées inviolables à partir d'une clé publique. Dans ce cas, il suffit bien sûr que l'émetteur et le destinataire de la clé chiffrée soient en mesure de mettre en oeuvre le procédé objet de l'invention à partir des paramètres secrets sur cette même clé publique, la transmission de cette dernière pouvant être librement accessible au public, et les paramètres secrets étant soit transmis de façon sûre, soit stockés sur un support inviolable, du genre carte à mémoire, et adressés tant à l'émetteur qu'au destinataire, pour appliquer le même traitement.

On a ainsi décrit un procédé et un dispositif de sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable, de très haute performance. Les hautes performances du procédé et du dispositif objet de l'invention concernent la solidité cryptographique de la signature élaborée, conformément au procédé de la présente invention. Cette solidité cryptographique apparaît résulter du fait qu'un texte donné peut engendrer sensiblement n'importe quelle signature ou sceau. Dans ces conditions, seule une recherche exhaustive permettrait de calculer la clef secrète à partir d'un texte et de son sceau ou signature. Le procédé et le dispositif objet de l'invention sont en outre remarquables en ce que un texte déterminé peut engendrer n'importe quelle signature, cette propriété apparaissant comme une garantie supplémentaire de solidité

cryptographique. En outre, l'algorithme de signature
est une fonction non commutative des données. Si
l'on modifie n'importe quel sous-ensemble des données,
celui-ci fût-il réduit à unchiffre, la signature sera
5 totalement différente. Le procédé et le dispositif
objet de l'invention peuvent en particulier être mis
en oeuvre dans le cas de la transmission de données
comptables telles que par exemple les données relatives
10 à la compensation bancaire. Le choix d'une taille de
signature, c'est-à-dire d'un nombre de caractères
suffisant, exclut pratiquement une recherche exhaus-
tive des clefs secrètes.

REVENDICATIONS

1. Procédé de sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable, caractérisé en ce qu'il consiste:

5 - à établir une signature chiffrée représentative des informations et de l'identité du détenteur desdites informations au moyen d'un algorithme de calcul, et à enregistrer celle-ci sur le support desdites informations,

10 - à enregistrer les paramètres de calcul de ladite signature sur au moins un support inviolable.

2. Procédé selon la revendication 1, caractérisé en ce que l'algorithme de calcul est un algorithme de chiffrement et de compression des informations à sauvegarder à partir d'au moins une clef secrète associée au signataire détenteur des informations.

15 3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que le support inviolable est constitué par une carte à mémoire protégée.

20 4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que en vue d'assurer la transmission des informations sauvegardées selon l'une des revendications précédentes à un destinataire, ledit procédé consiste :

25 - à adresser ledit support inviolable sur lequel les paramètres de calcul de la signature chiffrée sont enregistrés audit destinataire,

- à transmettre lesdites informations sauvegardées et la signature chiffrée audit destinataire.

30 5. Procédé selon la revendication 4, caractérisé en ce que en vue de contrôler le contenu des données transmises et reçues par le destinataire ledit procédé consiste en outre, à partir des paramètres de calcul de ladite signature chiffrée contenus dans le support inviolable,

- à établir une signature chiffrée de contrôle S' à partir des informations sauvegardées reçues suite à la transmission,
- à comparer ladite signature chiffrée reçue par transmission et ladite signature chiffrée de contrôle, l'identité des informations sauvegardées et des informations reçues par le destinataire et l'origine authentifiée de ces informations étant obtenues à la coïncidence de la signature chiffrée et de la signature chiffrée de contrôle.

5 6. Procédé selon l'une des revendications 1 à 5, caractérisé en ce que la clef secrète constituant au moins une partie des paramètres de calcul de ladite signature est enregistrée dans la zone protégée d'un support inviolable, ledit support inviolable étant à la disposition du détenteur des informations à sauvegarder et/ou du destinataire.

10 7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que ladite clef secrète et la signature sont constituées par un mot comprenant un nombre de caractères identiques.

15 8. Procédé selon l'une des revendications précédentes, caractérisé en ce que la signature et/ou la clef est constituée par un mot comprenant des caractères alpha-numériques.

20 9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que en vue d'établir ladite signature chiffrée représentative des informations et de l'identité du détenteur des informations, ledit algorithme de chiffrement consiste :

25 - à initialiser la création d'une suite de nombres aléatoires ou pseudo-aléatoires à plusieurs chiffres à partir de la ou des clefs secrètes, ladite

suite de nombres comportant un même nombre de termes (Ci) que le nombre de caractères (Ii) de l'information à sauvegarder,

5 - à effectuer le produit scalaire (P) terme à terme de la suite de nombres aléatoires (Ci) et de l'information à sauvegarder (Ii),

$$P = \sum_{i=1}^N I_i * C_i$$

10 - à effectuer une réduction modulaire du produit scalaire modulo p, de façon à définir un nombre A = Pmodulo p dans lequel p est un nombre premier comportant un nombre de chiffres égal au nombre de caractères de la ou des clefs secrètes ou de la signature,

15 - à effectuer une exponentiation modulaire du nombre A de façon à définir un nombre S = A^e_d modulo q, dans lequel q est un autre nombre premier comportant un nombre de chiffres égal aux nombres de caractères de la ou des clefs secrètes ou de la signature, et d un ou plusieurs chiffres de la clé ou des clefs secrètes, le nombre S constituant la signature chiffrée.

20 10. Procédé selon la revendication 9, caractérisé en ce que au produit scalaire P est ajoutée une valeur aléatoire produit de nombres supplémentaires aléatoires ou pseudo-aléatoires CN + k et de valeurs numériques arbitraires telles que la date, l'heure, un numéro d'identification du détenteur d'informations ou nombre aléatoire.

25 11. Procédé selon la revendication 9, caractérisé en ce que aux caractères (Ii) de l'information à sauvegarder sont ajoutés, par concaténation, des chaînes de caractères représentatives de valeurs numériques significatives arbitraires telles que la date,

l'heure, un numéro d'identification du détenteur d'informations ou nombre aléatoire.

12. Procédé selon l'une des revendications 9 à 11, caractérisé en ce que lesdites informations à sauvegarder (I_i) et les nombres aléatoires (C_i) sont subdivisés en blocs (B_j) contenant un nombre déterminé Q de caractères, le produit scalaire P étant calculé pour chacun des blocs (B_j) de façon à définir des produits scalaires partiels

$$P_j = \sum_i^Q I_i * C_i .$$

13. Procédé selon la revendication 12, caractérisé en ce qu'une signature partielle (S_j) est calculée pour chacun des blocs (B_j), la suite des signatures (S_j) constituant la signature représentative de l'ensemble des informations à sauvegarder.

14. Procédé selon l'une des revendications 9 à 13, caractérisé en ce que les nombres aléatoires ou pseudo-aléatoires (C_i) sont des nombres comportant un nombre l de chiffres ou caractères égal au nombre de caractères de la clef, les caractères (I_i) de l'information à sauvegarder étant groupés de façon que le nombre de chiffres de chaque terme C_i de la suite soit supérieur au nombre de caractères constituant un groupement.

15. Procédé selon l'une des revendications 1 à 14, caractérisé en ce que pour une même quantité d'information à sauvegarder $\sum_i I_i$, ledit procédé consiste à calculer de manière itérative une pluralité (r) de signatures (S_K) successives, lesdites signatures (S_{K-1}) étant successivement intégrées à l'information à sauvegarder $\sum_i I_i + \sum_k S_k$ pour calculer la signature d'ordre supérieur S_K .

16. Procédé selon l'une des revendications

1 à 15, caractérisé en ce que préalablement à son inscription sur le support des informations (Ii) ou sur le support inviolable ladite signature (S) est soumise en outre à un traitement de chiffrement à partir d'une clef secrète de chiffrement de façon à obtenir une signature chiffrée (Sc) présentant un nombre de caractères identique à celui de la signature.

17. Dispositif pour la sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable, caractérisé en ce qu'il comprend :

- des premiers moyens de mémorisation (101) dans lesquels sont mémorisées la ou les clefs secrètes du détenteur signataire ou du destinataire des informations,

- des deuxièmes moyens de mémorisation (102) dans lesquels est mémorisé un programme de calcul d'une ou plusieurs signatures (S, Sc) selon l'une des revendications 1 à 16 précédentes,

- des moyens de calcul (103) de la ou des signatures (S', Sc) et d'inscription (104) de ces signatures (S, Sc) sur le support des informations (Ii) à sauvegarder,

- des moyens de comparaison (105) de la signature (S, Sc) inscrite sur le support des informations avec la signature calculée,

- des moyens de validation (106) d'utilisation des informations sauvegardées sur coïncidence de la signature (S, Sc) calculée et de la signature enregistrée sur le support d'enregistrement des informations (Ii),

- des moyens périphériques (107) de saisie et/ou de visualisation des données.

18. Dispositif selon la revendication 17, caractérisé en ce que les premiers et deuxièmes 5 moyens de mémorisation sont constitués par des supports de mémorisation inviolables.

19. Dispositif selon la revendication 18, caractérisé en ce que les supports de mémorisation inviolables sont constitués par des cartes à mémoire protégée.

20. Dispositif selon l'une des revendications 17 à 19, caractérisé en ce qu'il est constitué par un ordinateur ou microordinateur.

21. Dispositif selon l'une des revendications 15 17 à 19, caractérisé en ce que les moyens périphériques consistant en un terminal de visualisation du genre "Minitel" ledit dispositif comprend en outre : 20 - un lecteur de cartes à mémoire protégée, - une cartouche enfichable comportant des mémoires mortes dans lesquelles est stocké le programme de calcul de la signature (S,Sc).

22. Dispositif selon l'une des revendications 19 à 21, caractérisé en ce que ladite signature (S,Sc) étant soumise en outre à un traitement de chiffrement conformément à la revendication 16 précédente, un 25 programme de chiffrement est mémorisé dans les zones protégées du support de mémorisation inviolable, le calcul de chiffrement de la signature S étant réalisé au sein de la carte à mémoire.

30 23. Dispositif selon l'une des revendications 17 à 22, caractérisé en ce qu'il comporte en mémoire permanente un programme de gestion de type "menu"

permettant sur incitation de l'utilisateur signataire par affichage de pages écran de dialogue interactif :

- d'introduire le code personnel de l'utilisateur signataire ou destinataire,

5 - d'introduire des paramètres arbitraires ou aléatoires tels que la date, l'heure ou des chiffres aléatoires,

- d'introduire l'information (Σ II) à sauvegarder.

10 24. Dispositif selon la revendication 23, caractérisé en ce que le programme de gestion de type "menu" permet en outre à un utilisateur :

- d'introduire la signature à vérifier pour comparaison à la signature stockée ou transmise,

15 - d'afficher la validation de cette signature.

25 25. Dispositif selon l'une des revendications 23 ou 24, caractérisé en ce que lesdites pages écran comportent une page écran de signalisation de risque de destruction de zones mémoires du support inviolable après un nombre déterminé d'essais infructueux de validation de signature.

20 26. Dispositif selon l'une des revendications 24 ou 25, caractérisé en ce que les procédures de signature et de validation de signature sont séparées, la procédé de validation de signature étant conditionnellement autorisée pour des codes d'identification de l'utilisateur identifiant distincts des codes d'identification de l'utilisateur signataire.

25 30 27. Dispositif selon l'une des revendications 17 à 26, caractérisé en ce que pour un nombre aléatoire d'identification déterminé introduit par l'utilisateur, possédant le code d'identification, l'intro-

duction d'une pseudo information à sauvegarder consistant en une répétition à l'identique des caractères (Ii) sur un nombre arbitraire de caractères permet d'engendrer un code d'accès aléatoire inviolable temporaire représentatif de cet utilisateur.

5 28. Dispositif selon la revendication 27, caractérisé en ce que sur transmission du code d'identification et du nombre aléatoire d'identification à un utilisateur récepteur, la procédure de validation du code d'accès aléatoire inviolable temporaire est autorisée.

10

REVENDICATIONS MODIFIEES

[reçues par le Bureau international le 24 juillet 1987 (24.07.87);
revendications originales 1 et 2 remplacées par nouvelle revendication 1;
revendication 2 supprimée; autres revendications inchangées mais renommérotées 1-27 (1 page)]

- 5 1. Procédé de sauvegarde qualitative d'informations numérisées enregistrées sur un support effaçable ou modifiable, consistant à établir une signature chiffrée représentative des informations et de l'identité du détenteur desdites informations au moyen d'un algorithme de calcul, et à enregistrer celle-ci sur le support desdites informations, caractérisé en ce que ledit procédé consiste à enregistrer les paramètres de calcul de ladite signature sur au moins un support inviolable, l'algorithme de calcul étant un algorithme de chiffrement et de compression des informations à sauvegarder à partir d'au moins une clef secrète associée au signataire détenteur des informations.
- 10 2. Procédé selon la revendication 1, caractérisé en ce que le support inviolable est constitué par une carte à mémoire protégée.
- 15 3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que en vue d'assurer la transmission des informations sauvegardées selon l'une des revendications précédentes à un destinataire, ledit procédé consiste :
 - 20 - à adresser ledit support inviolable sur lequel les paramètres de calcul de la signature chiffrée sont enregistrés audit destinataire,
 - à transmettre lesdites informations sauvegardées et la signature chiffrée audit destinataire.
- 25 4. Procédé selon la revendication 3, caractérisé en ce que en vue de contrôler le contenu des données transmises et reçues par le destinataire, ledit procédé consiste en outre, à partir des paramètres de calcul de ladite signature chiffrée contenu dans le support inviolable :

1/5

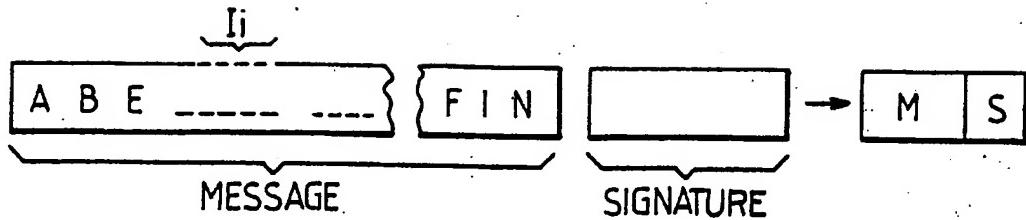


FIG-1

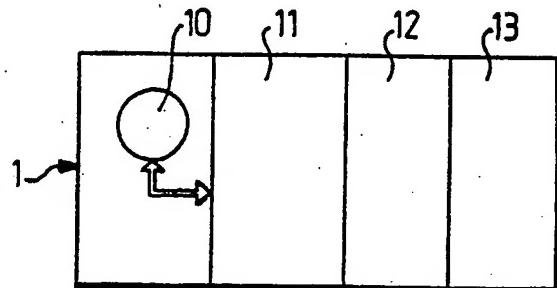


FIG-2

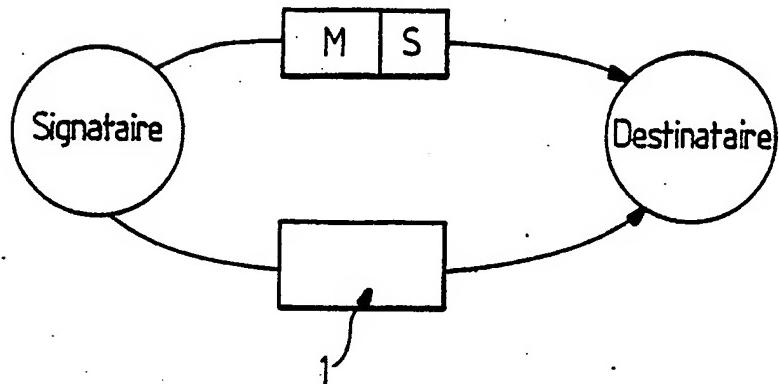
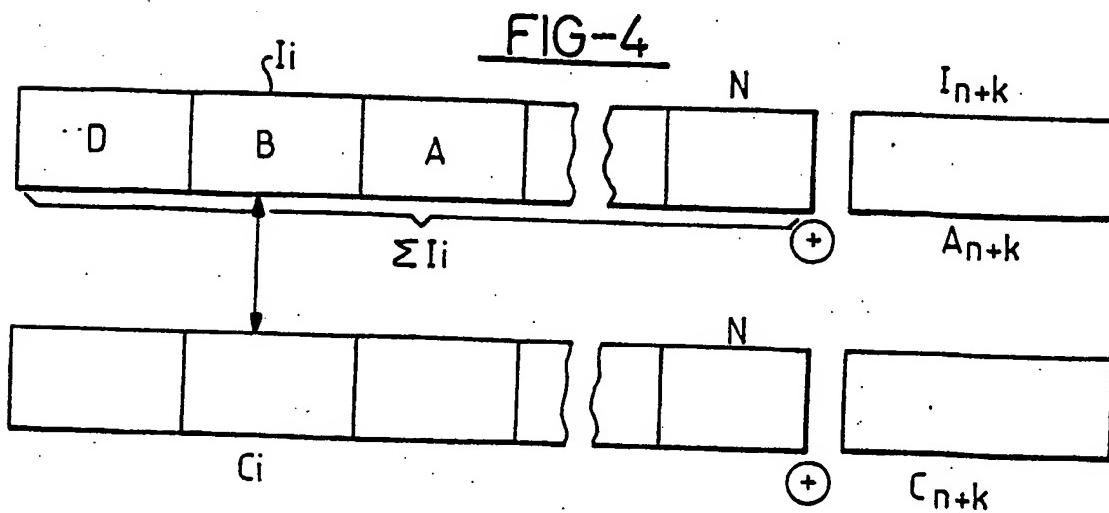
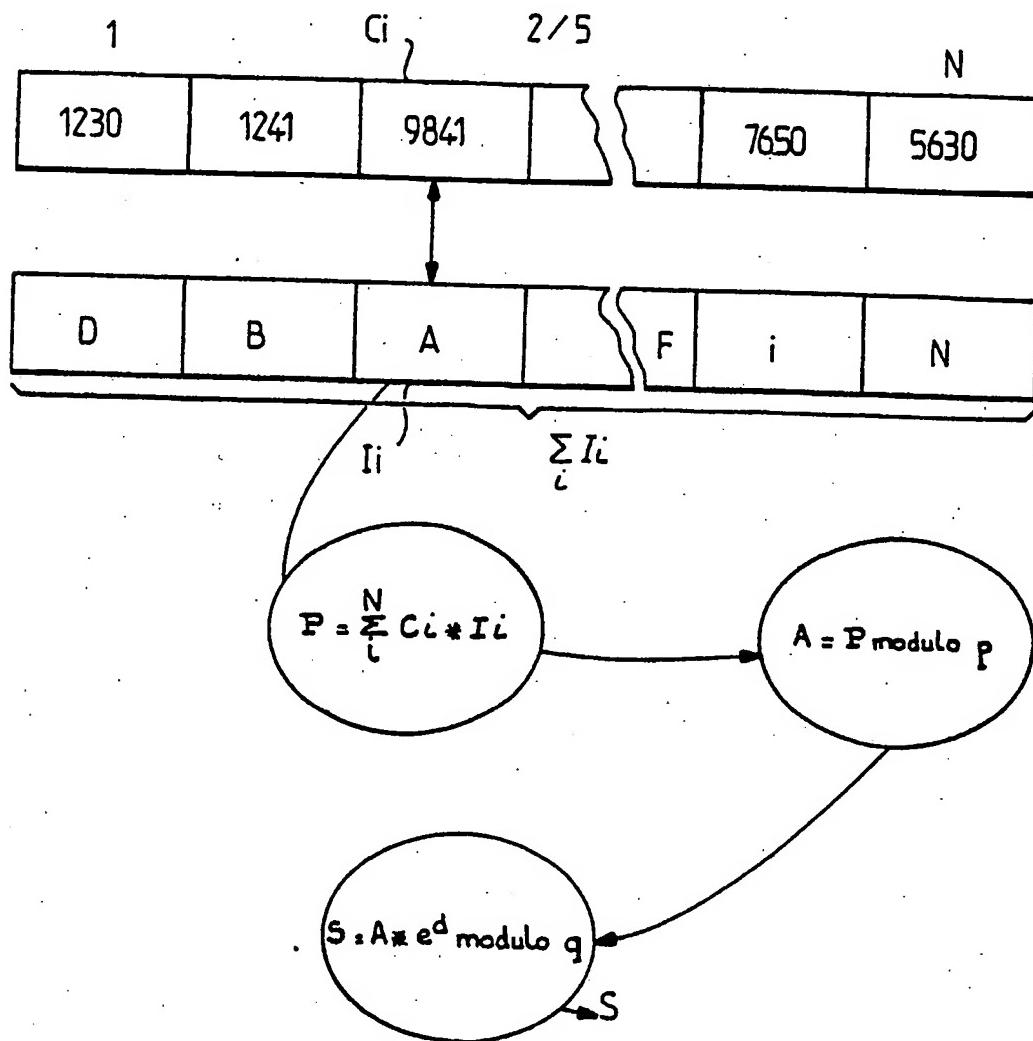
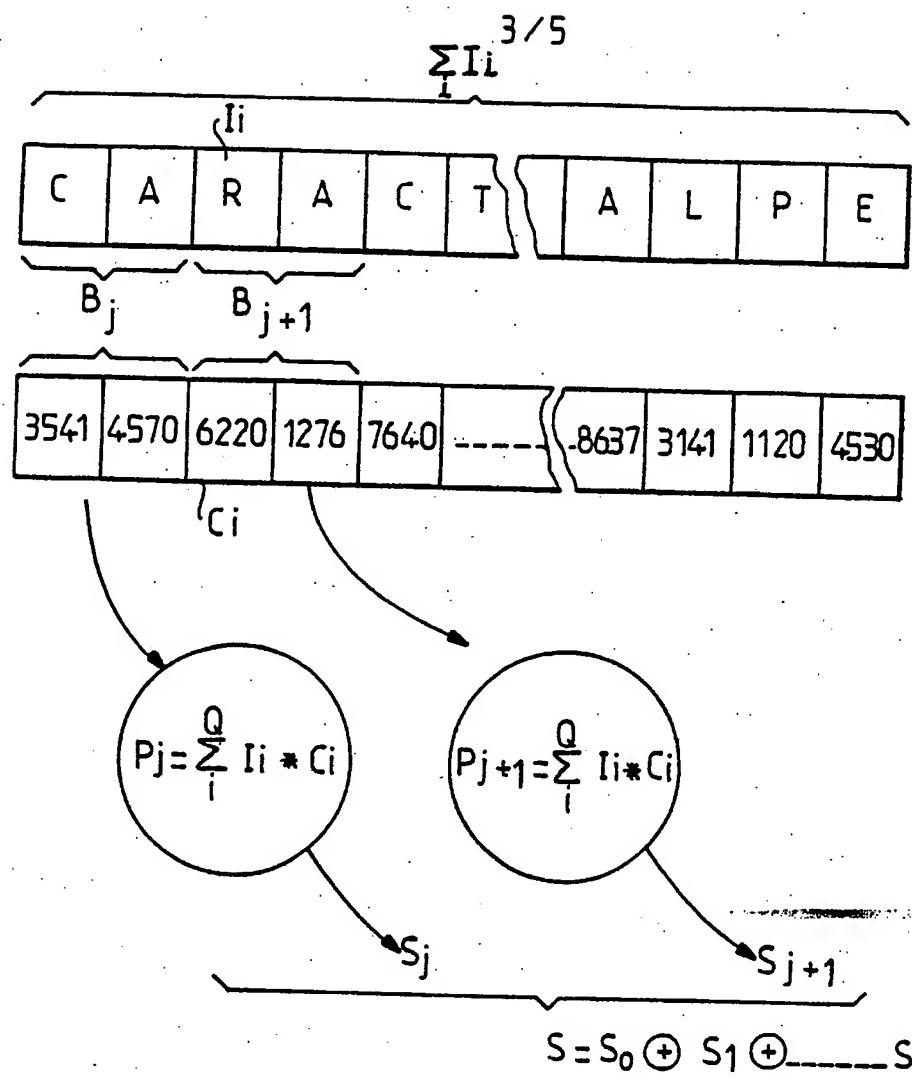
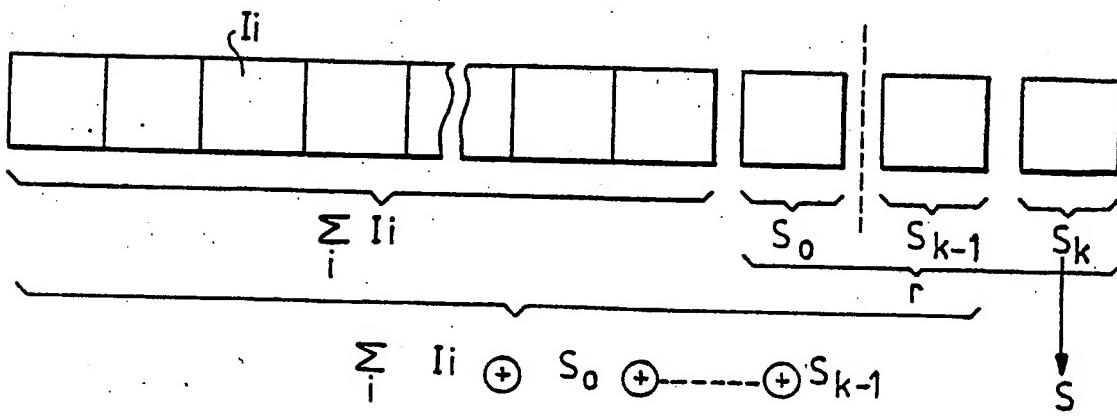
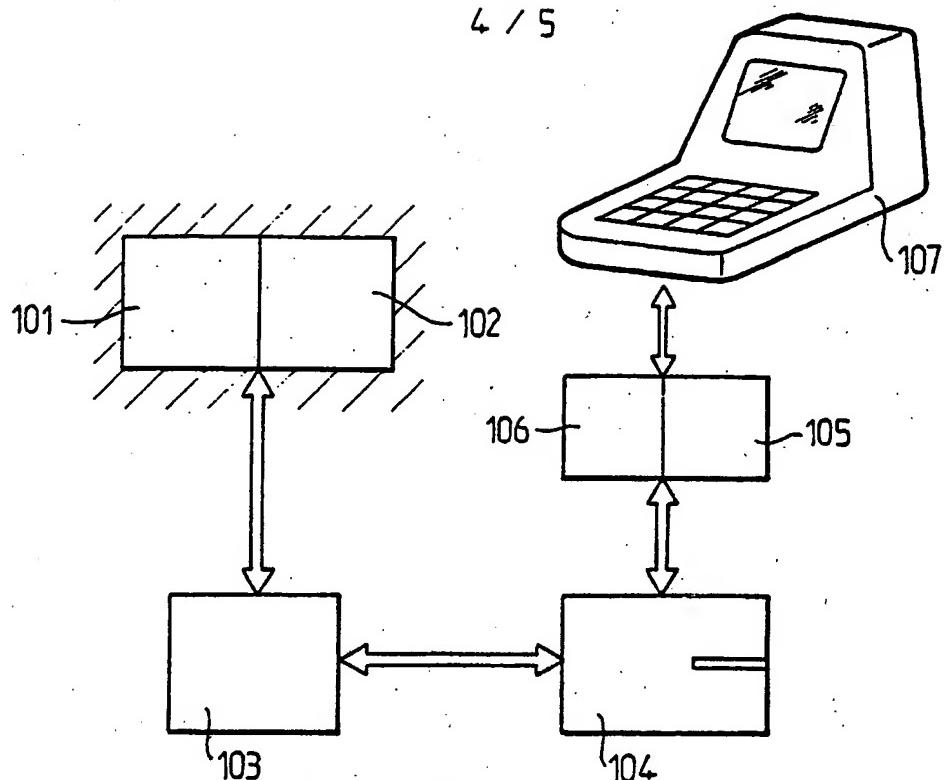
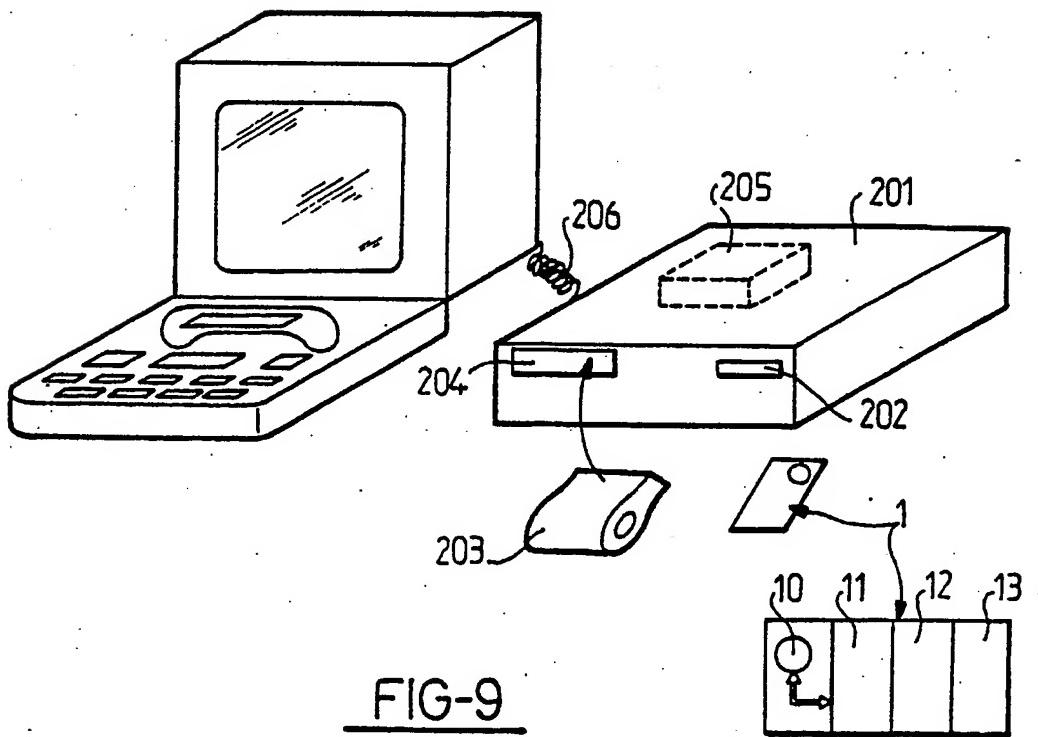


FIG-3

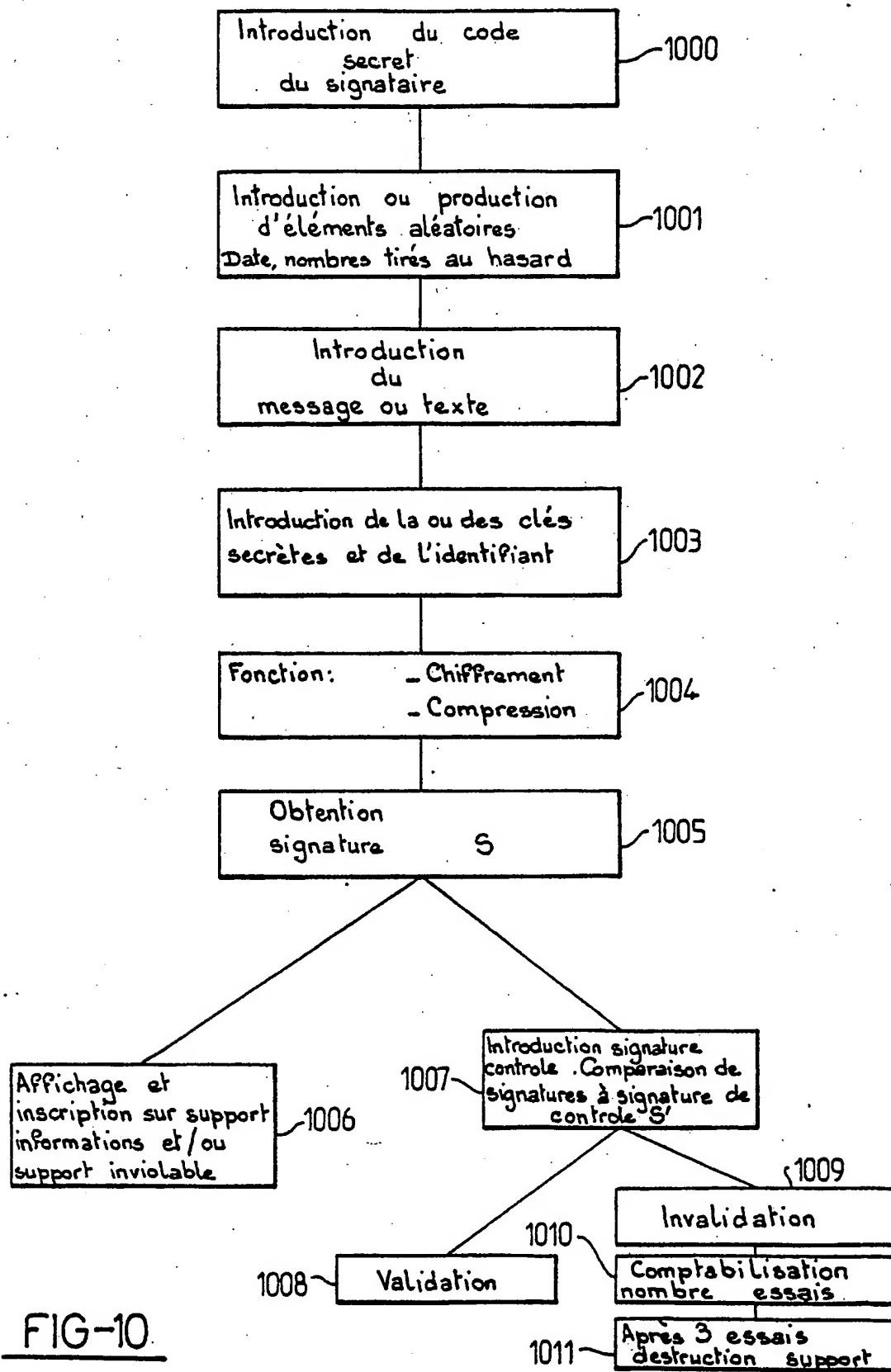
FIG-5

FIG-6FIG-7

4 / 5

FIG-8FIG-9

5 / 5

FIG-10

INTERNATIONAL SEARCH REPORT

International Application No PCT/FR 87/00079

I. CLASSIFICATION OF SUBJECT MATTER (If several classification symbols apply, indicate all) *	
According to International Patent Classification (IPC) or to both National Classification and IPC	

Int.Cl. ⁴: G 06 F 12/14; G 07 F 7/10

II. FIELDS SEARCHED	
----------------------------	--

Minimum Documentation Searched ⁷

Classification System	Classification Symbols
Int.Cl. ⁴	G 06 F 12/14; G 06 F 1/00; G 07 F 7/10

Documentation Searched other than Minimum Documentation
to the Extent that such Documents are Included in the Fields Searched ⁸

III. DOCUMENTS CONSIDERED TO BE RELEVANT*	
--	--

Category *	Citation of Document, ¹¹ with indication, where appropriate, of the relevant passages ¹²	Relevant to Claim No. ¹³
Y	EP, A1, 0089876 (CII HONEYWELL BULL), 28 September 1983, see figures; page 5, line 15 - page 9, line 11 --	1-6,17-20, 22
Y	GB, A, 2140179 (AMERICAN EXPRESS), 21 November 1984, see figure 4; page 6, line 55 - page 7, line 22 --	1-6,17-20, 22 11
A	US, A, 4211919 (UGON) 08 July 1980, see figures 1,2,5; column 6, line 34 - column 7, line 37 --	1,3,17
A	GB, A, 2163577 (NATIONAL RESEARCH DEVELOPMENT CORP.) 26 February 1986, see figure 1; page 2, line 120 - page 3, line 43 --	1,3,17
A	FR, A, 2266222 (MORENO) 24 October 1975 cited in the application -----	3

* Special categories of cited documents: ¹⁰

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the International filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the International filing date but later than the priority date claimed

"T" later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION	
--------------------------	--

Date of the Actual Completion of the International Search

15 May 1987 (15.05.87)

Date of Mailing of this International Search Report

12 June 1987 (12.06.87)

International Searching Authority

EUROPEAN PATENT OFFICE

Signature of Authorized Officer

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON

INTERNATIONAL APPLICATION NO. PCT/FR 87/00079 (SA 16522)

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 02/06/87

The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A- 0089876	28/09/83	FR-A- 2523745 JP-A- 58176746	23/09/83 17/10/83
GB-A- 2140179	21/11/84	None	
US-A- 4211919	08/07/80	FR-A, B 2401459 GB-A, B 2004394 DE-A- 2837201 JP-A- 54046447 US-A- 4295041 CH-A- 631561 JP-A- 62070993	23/03/79 28/03/79 01/03/79 12/04/79 13/10/81 13/08/82 01/04/87
GB-A- 2163577	26/02/86	EP-A- 0175487 US-A- 4634807	26/03/86 06/01/87
FR-A- 2266222	24/10/75	NL-A- 7503554 NL-A- 7503555 DE-A, B 2512902 DE-A, C 2512935 BE-A- 827137 BE-A- 827138 US-A- 3971916 US-A- 4007355 CH-A- 585933 GB-A- 1504196 GB-A- 1505715 JP-A- 51015946 JP-A- 51015947 CA-A- 1060582 CA-A- 1060583 SE-B- 406377 SE-A- 7503389 SE-A- 7503390 DE-C- 2560080	29/09/75 29/09/75 02/10/75 09/10/75 25/09/75 25/09/75 27/07/76 08/02/77 15/03/77 15/03/78 30/03/78 07/02/76 07/02/76 14/08/79 14/08/79 05/02/79 26/09/75 26/09/75 04/09/86

For more details about this annex :
see Official Journal of the European Patent Office, No. 12/82

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale N° PCT/FR 87/00079

I. CLASSEMENT DE L'INVENTION (si plusieurs symboles de classification sont applicables, les indiquer tous) ⁷

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

CIB⁴ : G 06 F 12/14; G 07 F 7/10

II. DOMAINES SUR LESQUELS LA RECHERCHE A PORTÉ

Documentation minimale consultée ⁸

Système de classification	Symboles de classification
CIB⁴	G 06 F 12/14; G 06 F 1/00; G 07 F 7/10

Documentation consultée autre que la documentation minimale dans la mesure où de tels documents font partie des domaines sur lesquels la recherche a porté ⁹

III. DOCUMENTS CONSIDÉRÉS COMME PERTINENTS ¹⁰

Catégorie ¹¹	Identification des documents cités, ¹¹ avec indication, si nécessaire, des passages pertinents ¹²	N° des revendications visées ¹³
Y	EP, A1, 0089876 (CII HONEYWELL BULL) 28 septembre 1983, voir figures; page 5, ligne 15 - page 9, ligne 11 --	1-6,17-20, 22
Y	GB, A, 2140179 (AMERICAN EXPRESS). 21 novembre 1984, voir figure 4; page 6, ligne 55 - page 7, ligne 22	1-6,17-20, 22
A	--	11
A	US, A, 4211919 (UGON) 8 juillet 1980, voir figures 1,2,5; colonne 6, ligne 34 - colonne 7, ligne 37	1,3,17
A	GB, A, 2163577 (NATIONAL RESEARCH DEVELOPMENT CORP.) 26 février 1986, voir figure 1; page 2, ligne 120 - page 3, ligne 43	1,3,17
A	FR, A, 2266222 (MORENO) 24 octobre 1975 cité dans la demande	3
<hr/>		

* Catégories spéciales de documents cités: ¹¹

- « A » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- « E » document antérieur, mais publié à la date de dépôt international ou après cette date
- « L » document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- « O » document se référant à une divulgarion orale, à un usage, à une exposition ou tous autres moyens
- « P » document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

« T » document ultérieur publié postérieurement à la date de dépôt international ou à la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

« X » document particulièrement pertinent: l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive

« Y » document particulièrement pertinent: l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier.

« & » document qui fait partie de la même famille de brevets

IV. CERTIFICATION

Date à laquelle la recherche internationale a été effectivement achevée

15 mai 1987

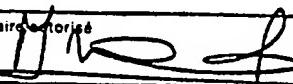
Administration chargée de la recherche internationale

OFFICE EUROPEEN DES BREVETS

Date d'expédition du présent rapport de recherche internationale

12 JUN 1987

Signature du fonctionnaire autorisé

M. VAN MOL 

ANNEXE AU RAPPORT DE RECHERCHE INTERNATIONALE RELATIF

A LA DEMANDE INTERNATIONALE NO. PCT/ER 87/00079 (SA 16522)

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche international visé ci-dessus. Lesdits membres sont ceux contenus au fichier informatique de l'Office européen des brevets à la date du 02/06/87.

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevets	Date de publication
EP-A- 0089876	28/09/83	FR-A- 2523745 JP-A- 58176746	23/09/83 17/10/83
GB-A- 2140179	21/11/84	Aucun	
US-A- 4211919	08/07/80	FR-A,B 2401459 GB-A,B 2004394 DE-A- 2837201 JP-A- 54046447 US-A- 4295041 CH-A- 631561 JP-A- 62070993	23/03/79 28/03/79 01/03/79 12/04/79 13/10/81 13/08/82 01/04/87
GB-A- 2163577	26/02/86	EP-A- 0175487 US-A- 4634807	26/03/86 06/01/87
FR-A- 2266222	24/10/75	NL-A- 7503554 NL-A- 7503555 DE-A,B 2512902 DE-A,C 2512935 BE-A- 827137 BE-A- 827138 US-A- 3971916 US-A- 4007355 CH-A- 585933 GB-A- 1504196 GB-A- 1505715 JP-A- 51015946 JP-A- 51015947 CA-A- 1060582 CA-A- 1060583 SE-B- 406377 SE-A- 7503389 SE-A- 7503390 DE-C- 2560080	29/09/75 29/09/75 02/10/75 09/10/75 25/09/75 25/09/75 27/07/76 08/02/77 15/03/77 15/03/78 30/03/78 07/02/76 07/02/76 14/08/79 14/08/79 05/02/79 26/09/75 26/09/75 04/09/86

Pour tout renseignement concernant cette annexe :
voir Journal Officiel de l'Office européen des brevets, No. 12/82

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.